

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**



AIR FORCE INSTRUCTION 14-119

4 MAY 2012

Incorporating Through Change 2,

31 March 2016

Intelligence

***INTELLIGENCE SUPPORT TO FORCE
PROTECTION (FP)***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AMC/A2

Certified by: AF/A2D
(Brig Gen Thomas W. Geary)

Supersedes: AFI 14-119, 15 August 2007

Pages: 25

This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources and Operations* and AFPD 14-2, *Intelligence Rules and Procedures*, and incorporates guidance from Air Force Instruction (AFI) 14-104, *Oversight of Intelligence Activities*, AFI 14-202 Volume 1, *Intelligence Training*, AFI 14-202 Volume 2, *Intelligence Standardization/Evaluation Program*, AFI 14-202 Volume 3, *General Intelligence Rules*, and AFI 31-101, *Integrated Defense*. This publication defines intelligence support requirements to Force Protection. It applies to Regular Component, Air Force Reserve (AFR), Air National Guard (ANG), and Department of the Air Force (AF) Civilians. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct supplements are routed to the OPR of this publication for coordination prior to certification and approval. Major Commands (MAJCOMs) need to provide a copy to the OPR upon publication. IAW Air Force Instruction (AFI) 33-360, *Publication and Forms Management*, the authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of

command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items.

SUMMARY OF CHANGES

This interim change transfers OPR from Air Staff (AF/A2DX) to Air Mobility Command (AMC) and updates AF/A2 roles accordingly. The MAJCOM requirement to submit an annual report describing their FP Intelligence program has been eliminated. No new requirements are introduced in this Interim Change. The term IPB has replaced IPOE in order to parallel Joint Service terminology. Additionally, paragraphs were removed that duplicate guidance already contained in AFI 14-202 volumes and others were reworded to eliminate ambiguity. A margin bar (|) indicates newly revised material.

Chapter 1— OVERVIEW	4
1.1. Threat Environment.	4
1.2. Intelligence Support to Force Protection (ISFP).	4
1.3. Force Protection Intelligence (FPI) is analyzed, all-source intelligence information that, when integrated or fused with other FP information, provides an assessment of the threats to DoD missions, people or resources.	4
1.4. DELETED	4
1.5. Adhering to guidance in Department of Defense Instruction (DoDI) 2000.	4
1.6. Intelligence supports FP directly through unit deployments, readiness training, mission planning support, and threat analysis.	4
Chapter 2— ROLES AND RESPONSIBILITIES	6
2.1. The Air Force Office of Special Investigations (AFOSI).	6
2.2. Deputy Chief of Staff (DCS) for Logistics, Installations and Mission Support (AF/A4) and Director of Security Forces AF/A4S.	6
2.3. Deputy Chief of Staff (DCS) for Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2) and Directorate of Intelligence, Surveillance and Reconnaissance Strategy, Plans, Policy and Force Development (AF/A2D).	6
2.4. MAJCOM Directors of Intelligence (A2) Responsibilities.	7
2.5. Host Unit (In-garrison) Intelligence Responsibilities.	9
2.6. Expeditionary Intelligence Responsibilities.	13
2.7. Tenant Unit Intelligence Responsibilities.	15

Chapter 1

OVERVIEW

1.1. Threat Environment. All Airmen are subject to threats whether in the continental United States (CONUS), outside the continental United States (OCONUS) or deployed to expeditionary bases. Asymmetric threats and hazards, including those from insiders (as addressed in AF Doctrine ANNEX 3-10), will increasingly challenge US personnel, facilities and assets. **Note:** The USAF definition of FP (AF Core Doctrine, Volume Five – SUPPORT, Chapter Four – Protect Forces) includes all hazards, but this expanded definition does not expand the Intel support mission to include all hazards. Understanding how these threats and hazards affect the mission is the first step toward developing an effective FP program that will help commanders assess their ability to deter, pre-empt, negate or mitigate hostile actions or events.

1.2. Intelligence Support to Force Protection (ISFP). Tailored, focused Intelligence Support to Force Protection (ISFP) assists commanders and other force-protection responsible personnel by providing robust threat intelligence/information access and analysis, cross-career field collaboration, and fusion. Intelligence personnel must be organized, trained and equipped to support the FP mission and FP customers as required.

1.3. Force Protection Intelligence (FPI) is analyzed, all-source intelligence information that, when integrated or fused with other FP information, provides an assessment of the threats to DoD missions, people or resources. FPI is proactive and drives FP decisions in support of the commander's intent.

1.4. DELETED

1.5. Adhering to guidance in Department of Defense Instruction (DoDI) 2000. 16, *Antiterrorism (AT) Standards*. FP assessments are performed collaboratively by intelligence, Air Force Office of Special Investigations (AFOSI), and security forces (SF) personnel and in cooperation with several other entities. These entities include operations, weather, medical, communications, etc. FP customers include all personnel from commanders to airmen, but more tailored, specialized support can be provided to: commanders, aircrews, SF, explosive ordnance disposal (EOD), civil engineers, medical personnel, antiterrorism officers (ATO), Phoenix Ravens/flyaway security teams, AFOSI, threat working groups (TWG), antiterrorism working groups (ATWG), integrated defense working groups (IDWG), base defense operations center (BDOC), CRG, or other associated units. FP information assessments should include all relevant information.

1.6. Intelligence supports FP directly through unit deployments, readiness training, mission planning support, and threat analysis. Intelligence also supports the Integrated Defense (ID), Critical Asset Risk Management (CARM), and indirectly, the Emergency Management elements of the FP mission. Outside the CONUS, intelligence collection activities target foreign adversaries. Within the CONUS, however, AFOSI works with federal, state, tribal and local law enforcement and intelligence agencies to identify, exploit and neutralize criminal, terrorist and foreign intelligence threats to the USAF, DoD, and US Government (USG). Generally, intelligence personnel provide the following support to FP operations:

1.6.1. Indications and warning (emerging crisis situations).

1.6.2. Current intelligence (adversary intentions, courses of action).

1.6.3. General military intelligence (adversary Order of Battle [OB], cultural awareness information).

1.6.4. Near-real-time/real-time situational awareness and understanding.

1.6.5. Intelligence Preparation of the Battlespace (IPB) (adversary capabilities and tactics, techniques and procedures [TTPs], terrorist group historical background and intent, SIPRNET and SCI message traffic, finished intelligence, terrain analysis, route analysis, man-portable air defense system [MANPADS]/stand-off weapons footprints, cyber threat, etc.). **Note:** This can be performed at all CONUS and OCONUS locations. Refer to AFI 14-104 for guidance on Intelligence Oversight considerations in regards to Intelligence Support to FP.

1.6.6. Geospatial Intelligence (GEOINT), target intelligence (maps, charts, imagery, target studies, and target folder development and, if appropriate, Measurement and Signature Intelligence (MASINT)).

1.6.7. Combat assessment (pre-/post-mission briefings/debriefings, mission assessments).

1.6.8. Scientific and technical intelligence (weapon characteristics, capabilities, vulnerabilities, limitations and effectiveness).

1.6.9. Force protection intelligence-related commander's critical information requirements (CCIR) and essential elements of information (EEI).

1.6.9.1. This AFI does not provide authorization for intelligence personnel to collect and maintain information on US persons without an authorized mission to do so. While Intelligence Oversight (IO) policy restricts collection of information on US persons to units with an authorized mission, it does not preclude intelligence personnel from receiving, viewing, fusing, analyzing or passing such information to the proper entity (SF or AFOSI) responsible for mitigating the threat. In most matters regarding US persons' information, intelligence personnel will defer to AFOSI in its role as a designated counterintelligence (CI) component. See AFI 14-104 for more information regarding restrictions and procedures on collecting information related to US persons.

1.6.9.2. DELETED

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. The Air Force Office of Special Investigations (AFOSI). IAW Air Force Mission Directive (AFMD) 39, *Air Force Office of Special Investigations*, AFOSI is the sole Air Force organization authorized to initiate and conduct counterintelligence investigations, operations, collections, and other related activities. In CONUS, AFOSI notifies and refers to the FBI those incidents and investigative matters meeting the criteria in Department of Defense Instruction (DoDI) 5240.04, *Counterintelligence Investigations*.

2.1.1. Within the Continental United States (CONUS), AFOSI works with federal, state, tribal and local law enforcement and intelligence agencies to identify, exploit and neutralize criminal, terrorist and foreign intelligence threats to the USAF, DoD, and US Government (USG). Generally speaking, AFOSI is the go to organization for CONUS-based FP-related threat information.

2.1.2. Outside the United States, AFOSI coordinates CI investigations according to intelligence community directives. Organizations may request AFOSI products and services from their servicing AFOSI field investigative region (FIR)/squadron/detachment (Det). Refer to AFI 71-101 Volume 4, *Counterintelligence*, for the full scope of responsibilities.

2.2. Deputy Chief of Staff (DCS) for Logistics, Installations and Mission Support (AF/A4) and Director of Security Forces AF/A4S. Serves as the primary advisor to the Chief of Staff of the Air Force (CSAF) for FP and Integrated Defense (ID) and acts as the approval authority for FP and ID guidance. SF is responsible for ID operations, synchronizing protection and defense efforts against all threats and hazards to AF installations. The SF squadron commander is the Defense Force Commander (DFC) and primary advisor on ID operations and installation security for the installation commander, and employs security force/ID force personnel to execute security operations. Refer to AFPD 31-1, *Integrated Defense* and AFI 31-101 for the full scope of responsibilities regarding ID.

2.3. Deputy Chief of Staff (DCS) for Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2) and Directorate of Intelligence, Surveillance and Reconnaissance Strategy, Plans, Policy and Force Development (AF/A2D). AF/A2 and AF/A2D will:

2.3.1. Provide policy for planning, programming, training, and budgeting resources necessary to ensure the AF has the capability to collect, analyze, produce and disseminate all-source intelligence information to support FP operations.

2.3.2. Coordinate on AF, DoD and Intelligence Community (IC) policies affecting FPI.

2.3.3. DELETED

2.3.4. DELETED

2.3.5. Collaborate with HQ AFOSI (SAF/IGX) and AF/A4S on FP information, policy, processes and assessments.

2.3.6. Deleted

2.3.7. Deleted

2.4. MAJCOM Directors of Intelligence (A2) Responsibilities. MAJCOM/A2s provide overall management of the command's ISFP responsibilities. The role of the MAJCOM/A2 is to provide guidance for intelligence training, ensure units have the materials needed to standardize ISFP, and assist units in conducting ISFP where necessary. MAJCOM/A2s will:

2.4.1. Coordinate FP-related products (i.e., daily intelligence summaries, terrorist handbooks, threat documents and briefings, etc.) and services with appropriate AFOSI regions, MAJCOM security forces and Operations personnel, appropriate HHQ critical asset risk management assessors, etc., to deconflict work responsibilities and ensure that customer requirements are satisfied.

2.4.1.1. Establish guidance for, program for, allocate resources for, and provide management for all command FP-related intelligence requirements. MAJCOMs should tailor the responsibilities listed in this paragraph based upon FP customer requirements, location and mission/area of operations.

2.4.1.2. Develop and implement an intelligence support to FP program in coordination with the supported Combatant Command (COCOM) air components, AFOSI Region, and MAJCOM staff elements (e.g., A3, A5 and A4).

2.4.1.3. Ensure MAJCOM policy on ISFP follows existing processes and guidance for FP legal considerations, Law of Armed Conflict (LOAC), and that IO reviews are incorporated.

2.4.1.3.1. DELETED

2.4.1.3.2. Ensure subordinate organizations incorporate ISFP scenario injects and requirements, as appropriate.

2.4.1.3.3. Establish procedures to rapidly receive, evaluate, analyze and disseminate all relevant intelligence threat data with AFOSI, SF and other Staff FP elements.

2.4.1.3.4. In coordination with AFOSI, analyze all-source intelligence and provide warning to FP customers including subordinate units and commanders, both in garrison and in transit.

2.4.1.3.5. DELETED

2.4.1.3.6. Participate in the MAJCOM ATWG, TWG and other working groups as set forth in AFI 10-245, and applicable COCOM guidance.

2.4.1.3.7. Incorporate operations/contingency and exercise lessons learned, trends and best practices into ISFP tactics, techniques and procedures.

2.4.1.4. DELETED

2.4.1.4.1. Deleted

2.4.1.4.2. Deleted

2.4.1.4.3. Deleted

2.4.1.4.4. Deleted

2.4.1.4.5. Deleted

2.4.1.4.6. Deleted

2.4.1.5. DELETED

2.4.1.6. DELETED

2.4.1.7. Establish compliance criteria that give clear guidance on unit programs and their expected results.

2.4.1.8. Provide intelligence FP Unit Type Code (UTC) management and inform the Air Staff Functional Manager of any FP UTC-related problems, as applicable. Provide assistance addressing contingency or exercise-related manpower, equipment and communication requirements. Provide list of minimum requirements for mobility equipment.

2.4.1.9. Assist AFOSI FIR/Det (refer to AFOSI's AFI 71-101, Vol 4) and supported COCOM in development of threat assessments.

2.4.1.10. IAW AFI 32-3001, *Explosive Ordnance Disposal Program*, MAJCOMs that have responsibility for EOD shall provide threat support and products for EOD programs.

2.4.1.11. Obtain customer feedback on intelligence products and services and disseminate feedback to originating publishing unit/agency. Use the feedback to implement changes or create new products to meet customer requirements.

2.4.1.12. DELETED

2.4.1.13. Manage ISFP collection and requirements.

2.4.1.13.1. Coordinate with AFOSI, SF and ISFP customers to jointly develop MAJCOM OCONUS FP-related PIRs that will serve to drive both theater and national ISR and CI collections.

2.4.1.13.2. Advocate enhanced production requirements of SECRET collateral-level, tear-line reporting to ensure the widest possible dissemination of FP threat information.

2.4.1.13.3. Oversee ISFP training support.

2.4.1.13.3.1. DELETED

2.4.1.13.3.2. DELETED

2.4.1.13.3.3. In coordination with FP customers, integrate the use of and/or update intelligence into FP customers' training courses, as applicable (e.g., Security Forces formal training courses and Regional Training Centers [RTCs], AT Level II Courses, Counter-Threat Operations Course, etc.).

2.4.1.13.3.4. When tasked, provide MAJCOM/A2-level comment on the AT Level II Course Curriculum.

2.4.1.13.3.5. DELETED

2.4.1.13.3.6. Annually, solicit formal unit intelligence FP training requirements (i.e., AT Level II, AF FP Intelligence Formal Training Unit (IFTU), etc.) for the subsequent year and coordinate requirements with appropriate agencies.

2.4.1.13.3.7. DELETED

2.5. Host Unit (In-garrison) Intelligence Responsibilities. Host units are all organizations with base operating support (BOS)/FP responsibilities for their in-garrison location.

2.5.1. Provide adequate in-garrison planning and direction (T-3).

2.5.1.1. Develop, implement and execute an FPI support program as an integral part of the installation commander's FP program. The program will identify which mission elements and functional areas, both at home and/or deployed, require intelligence support to perform their FP functions and tailor intelligence products to meet customer needs. (T-2)

2.5.1.1.1. Unless ISFP is the individual's primary duty, the Senior Intelligence Officer (SIO) will appoint, in writing, a primary and alternate officer, non-commissioned officer (NCO), civilian and/or contractor to provide intelligence support for FP (T-3). Unit intelligence personnel providing ISFP will have the appropriate security clearances consistent with the levels of the base/organization facilities (T-2). Where feasible, designated personnel should have access to Top Secret (TS), SCI, Human Intelligence (HUMINT) Control System (HCS) and Gamma (G) accredited work centers and information. It is advisable that an experienced intelligence professional be the primary designee to ensure that the designee has the scope of knowledge needed to be truly effective.

2.5.1.1.2. DELETED

2.5.1.1.3. Where authorized, Intelligence personnel assigned to the FP UTCs or designated by the SIO to support the base/unit Force Protection Program will attend FP IFTU. Work training requirements through the base/unit training manager of as directed by MAJCOM/A2 (T-2).

2.5.1.1.4. Designated personnel will participate in unit/base ATWGs, TWGs, FPWGs, and other functions (e.g., IDWG, IFC, TIFC, base defense operations center), as appropriate. (T-2)

2.5.1.2. Provide relevant intelligence threat information, products and services to subordinate units, to include geographically separated units (GSUs), units without an organic intelligence capability, AFRC-associated units and tenant units IAW MAJCOM guidance. (T-2)

2.5.1.3. Maintain sufficient communications and current POC listings to allow rapid contact with AFNORTH, MAJCOMs and units.

2.5.1.4. DELETED

2.5.1.5. Oversee FP training for intelligence personnel, including assigned/attached AF Reserve Component personnel, civilians, and contractors. (T-2)

2.5.1.6. DELETED

2.5.1.7. DELETED

2.5.1.8. DELETED

2.5.1.9. DELETED

2.5.1.10. DELETED

2.5.1.11. Review installation ID/AT plan at least annually and write an intelligence annex to identify all required intelligence support and information requirements.

2.5.1.12. DELETED

2.5.1.13. Establish and document procedures for providing intelligence products and services to FP customers.

2.5.1.14. In coordination with AFOSI and the Security Forces Squadron:

2.5.1.14.1. Analyze all-source intelligence information for impact on unit mission and rapidly disseminate threat information to subordinate and lateral units, HHQs and other appropriate agencies. (T-2)

2.5.1.14.2. Analyze all-source intelligence information focusing on enemy activities, capabilities, tactics, weapons, intentions and probable COAs throughout the Base Security Zone and provide support to FP customers through products and briefings. **Note:** For a thorough explanation of the Base Security Zone and the associated term Base Boundary, see AFPD 31-1 and AFI 31-101. Intelligence FP-support efforts must be focused on these areas. (T-2)

2.5.1.14.3. Establish procedures to track IC threat levels, threat warnings, alerts and advisories for threats at the home station, in deployed locations, or while in transit to deployed locations (based on approved FP plans submitted by assigned/attached units). (T-2)

2.5.1.15. Ensure continuity books are maintained (either electronic or hardcopy) and reviewed IAW local/unit guidance (T-3). Continuity books should include:

2.5.1.15.1. Appointment memo (for additional duty position).

2.5.1.15.2. AFI 14-2 (MDS) Volumes 1-3, AFI 14-202 Volumes 1-3, AFI 14-119, AFI 10-245 and MAJCOM supplements.

2.5.1.15.3. AF Tactics, Techniques and Procedures (AFTTP) 3-10.1, *Integrated Base Defense*.

2.5.1.15.4. Copies of intelligence FP products or templates (e.g., maps, overlays, MANPAD footprint, briefings).

2.5.1.15.5. Local operating instructions (if applicable).

2.5.1.15.6. Vulnerability assessment benchmarks.

2.5.1.15.7. Local TWG charter.

2.5.1.15.8. Nuclear Security Threat Capabilities Assessment (as appropriate).

2.5.1.15.9. FP customer requirements.

2.5.1.15.10. Intelligence portion of the installation ID/AT plan.

2.5.1.15.11. Installation and COCOM threat assessments.

2.5.1.15.12. FP CCIR and PIR list.

2.5.1.15.13. FP point of contact list.

2.5.1.15.14. IO Policy (e.g., AFI 14-104).

2.5.1.15.15. LOAC guidance.

2.5.1.16. DELETED

2.5.1.17. DELETED

2.5.1.18. Support/participate in lessons learned programs to identify and document ISFP findings, observations and best practices; update ISFP programs appropriately (T-3).

2.5.1.19. Support the annual development of AFOSI Local Threat Assessments (LTA). AFOSI may request intelligence support to ensure the LTA includes analysis of transnational/foreign terrorist TTPs, weapons (chemical, biological, radiological, nuclear, high-yield explosives [CBRNE], small arms, rocket propelled grenades [RPGs], MANPADS, improvised explosive devices [IEDs]), capabilities, activities, history, intent and probable COAs. (T-2)

2.5.1.20. Periodically publish and disseminate an accession list to FP customers incorporating all new, incoming FP/terrorism reference materials (e.g., websites/products).

2.5.1.21. Provide intelligence support and related activities (mission briefing, targeting, mission planning, GI&S support, FP threat updates, etc.) to transient units, as required.

2.5.1.22. IAW HHQ and MAJCOM guidance, assess and report each year on unit intelligence support to the FP program.

2.5.1.23. Actively solicit FP customer feedback to improve intelligence support processes, products and services. (T-2)

2.5.2. DELETED

2.5.2.1. DELETED

2.5.2.2. DELETED

2.5.3. Host Unit (in-garrison) Training Support.

2.5.3.1. Solicit and consolidate formal/special FP training requirements for all assigned and attached intelligence personnel.

2.5.3.2. IAW AFI 14-2 (MDS) Volume 3, AFI 14-202 Volumes 1-3 and MAJCOM guidance, establish an installation FP-focused intelligence training program tailored to the unit's mission, weapon system, projected contingency or AEF tasking and base/deployment locations.

2.5.3.2.1. Coordinate in writing, with AFOSI and FP customers to identify training requirements and develop an appropriate FP threat awareness program tailored to the unit's mission (T-2). Training programs should consider: 1) threat knowledge (as it applies to integrated defense), 2) visual recognition, 3) personnel recovery and 4) collection and reporting. Examples of FP threat awareness training topics include:

2.5.3.2.1.1. Terrorist TTPs, capabilities, activities, intentions.

2.5.3.2.1.2. Current threat, terrorism threat levels, advisories, alerts, warnings.

2.5.3.2.1.3. DELETED

2.5.3.2.1.4. MANPADS, RPGs, IEDs, CBRNE, rockets/mortars, small arms.

2.5.3.2.1.5. FP legal considerations (IO, Rules of Engagement) and the impact on OCONUS vs. CONUS operations. (T-2)

2.5.3.2.1.6. Locating FP threat data sources.

2.5.3.2.1.7. Post-mission debriefing requirements and procedures.

2.5.3.2.1.8. Intelligence support to FP capabilities and limitations.

2.5.3.2.2. Document how the FP threat awareness training program will be conducted. (T-2)

2.5.3.2.3. Provide a written evaluation of the FP threat awareness program to the appropriate leadership elements at the end of each annual training cycle. (T-2)

2.5.3.3. Establish an internal FP intelligence-training program (T-2). IAW MAJCOM guidance, establish minimum qualifications required for intelligence personnel to receive certification as FP threat awareness trainers. Ensure these trainers are certified in areas on which they provide instruction prior to the commencement of training. Actively solicit customer feedback to ensure that trainers meet program requirements.

2.5.3.3.1. DELETED

2.5.3.3.2. Individual training records shall be updated to reflect FP intelligence training IAW this publication and local instructions.

2.5.3.3.3. Internal FPI training programs should address all elements addressed in para. 5.1.3.2.1 above, as well as the following:

2.5.3.3.3.1. FP-focused predictive analysis (e.g., IPOE) and tailored threat assessments.

2.5.3.3.3.2. AFOSI, TWG, ATWG, fusion and BDOC roles/responsibilities.

2.5.3.3.3.3. Support to FP planning, programming and operations.

2.5.3.3.3.4. Support to VAs, ORIs, UCIs, NSIs, and exercises.

2.5.3.3.3.5. Support development of the installation LTA and develop an understanding of the Integrated Defense Risk Management Process (IDRMP).
Note: Training should be provided by the DFC staff.

2.5.3.3.3.6. Identification and use of FP threat data sources.

2.5.3.3.3.7. Detailed review of FPI legal considerations (IO, Rules of Engagement).

2.5.3.3.3.8. Familiarization with FP policy documents.

2.5.3.3.3.9. FP CCIRs, PIRs and customer requirement.

2.5.3.3.3.10. An understanding of the interaction between Intel and AFOSI roles/responsibilities.

2.6. Expeditionary Intelligence Responsibilities. This applies to units and /or personnel deploying in support of an AF FP support mission/operation. These responsibilities should be tailored to meet the needs of the deployed location based upon the mission, environment (permissive/hostile), threats, location, etc. Since expeditionary circumstances cannot be pre-determined, all deploying intelligence personnel should be adaptable to the environment. The SIO and intelligence personnel must be prepared to perform the duties listed below, and be prepared to coordinate terrorism-related and FISS products and services with AFOSI to deconflict responsibilities and thus ensure that customer requirements are satisfied (T-2).

2.6.1. Expeditionary Pre-deployment

2.6.1.1. DELETED

2.6.1.2. DELETED

2.6.1.3. DELETED

2.6.1.4. DELETED

2.6.1.5. DELETED

2.6.1.6. Submit pre-deployment FP intelligence requirements to servicing MAJCOM and coordinate necessary requirements with the appropriate theater and deployed SIOs.

2.6.1.7. DELETED

2.6.1.8. DELETED

2.6.1.9. DELETED

2.6.1.10. DELETED

2.6.1.11. DELETED

2.6.2. Expeditionary Collection and Requirements Management.

2.6.2.1. In coordination with TWG, IDWG, BDOC, or base defense operations, assist commanders in developing installation PIRs when applicable (T-3).

2.6.2.2. DELETED

2.6.2.3. In coordination with other deployed force protection elements, develop and coordinate collection requirements with theater collection managers (T-3).

2.6.3. Expeditionary Employment.

2.6.3.1. Ensure ISFP materials are available to support the Wing/Base/Installation/Defense Force Commander's FP Program (T-3).

2.6.3.2. Allocate, assign and manage all intelligence FP personnel resources. In a deployed environment, FP Intelligence UTCs are best used to provide qualified intelligence personnel to meet FP requirements. Intelligence personnel supporting FP operations and missions may be tactically controlled by the supported commander and administratively/operationally controlled by the installation/wing SIO.

2.6.3.3. Determine appropriate intelligence requirements/tasks with FP customers and coordinate support with AFOSI. Typical requirements could include: identification of enemy COAs and impact of asymmetric threats on air operations based on IPOE and

trends/event/link analysis; conducting MANPADS threats indirect/direct fire assessments; providing CBRNE, IEDs, ambush and kidnapping information; providing intelligence assessments; supporting the construction of targeting packages/target studies, route analyses, media/document exploitation; managing EEIs and production requirements; maintaining intelligence databases, systems and SSO programs; identifying unit support requirements and providing adhoc threat training; or similar requirements.

2.6.3.4. Conduct pre-mission briefings to support security forces during guard mount, and prior to ground patrols, convoy operations, counter-threat operations, and weapons storage area missions.

2.6.3.5. Conduct pre-mission briefings to support EOD operations. Develop procedures to assure that EOD activities produce timely reports that include all perishable, critical information of intelligence value.

2.6.3.6. Debrief FP and “outside-the-wire” operations IAW MAJCOM/theater directives and develop procedures to ensure ground teams provide timely reports that include all perishable, critical information of intelligence value, including FP information. Debrief EOD operations and review EOD post-blast analysis reports for potential FPI. Coordinate with AFOSI to ensure access to their post-mission personnel for debrief, as appropriate.

2.6.3.6.1. Ensure critical debrief information is disseminated rapidly to all appropriate organizations (e.g., AFOSI, DFC, ATO).

2.6.3.6.2. Follow up all voice reports with written documentation to ensure collected information is reintroduced into the intelligence cycle IAW HHQ/theater directives (e.g., mission report [MISREP], intelligence report [INTREP], spot report [SPOTREP], Intelligence Summaries [INTSUM], Situation Reports [SITREP]).

2.6.3.7. Develop quality control procedures to guarantee standardization and accuracy of situation/OB displays for FP considerations.

2.6.3.8. Ensure all organization FPI functions are equipped with the required GI&S, imagery and target material products to support briefings, mission planning, staff support and employment operations.

2.6.3.9. Ensure pre-planned missions are updated to reflect the latest available intelligence information affecting the mission, including FP updates, and are planned to minimize the threat and enhance survivability.

2.6.3.10. DELETED

2.6.3.11. Coordinate with FP customers to identify training requirements and develop an appropriate FP threat awareness program.

2.6.3.12. Participate in the TWG and other related functions (e.g., ATWG, BDOC, EMWG).

2.6.3.13. Analyze all-source intelligence for impact on unit missions and rapidly disseminate threat information to FP customers, subordinate and lateral units, HHQs and other appropriate agencies, in coordination with AFOSI.

2.6.3.14. Incorporate threat information into FP planning and operations.

2.6.3.15. Establish procedures to track and disseminate IC terrorism threat levels, terrorism warnings, alerts and advisories in coordination with AFOSI.

2.6.3.16. Ensure current FP checklists, templates, or procedures are available for expeditionary operations to include, as a minimum:

2.6.3.16.1. Intelligence support to mission planning.

2.6.3.16.2. OB displays.

2.6.3.16.3. Briefing and Debriefing procedures.

2.6.3.16.4. Reporting (e.g., mission report [MISREP], intelligence report [INTREP], spot report [SPOTREP], Intelligence Summaries [INTSUM], Situation Reports [SITREP]).

2.6.3.16.5. Automated intelligence systems operations and passwords.

2.6.3.16.6. Operational Security (OPSEC) requirements and procedures.

2.6.3.16.7. Threat awareness training.

2.6.3.17. Ensure that contingency continuity books are maintained (T-3).

2.6.3.17.1. DELETED

2.6.3.17.2. DELETED

2.6.3.17.3. DELETED

2.6.3.17.4. DELETED

2.6.3.17.5. DELETED

2.6.3.17.6. DELETED

2.6.3.17.7. DELETED

2.6.3.17.8. DELETED

2.6.3.18. DELETED

2.6.3.19. DELETED

2.6.3.20. DELETED

2.6.3.21. DELETED

2.6.3.22. DELETED

2.6.3.23. DELETED

2.7. Tenant Unit Intelligence Responsibilities.

2.7.1. The host unit with BOS responsibilities, whether AF or Joint, provides for the force protection of the installation and personnel.

2.7.2. Tenant units must ensure they are included on their host installation's FP plan through Memorandum of Agreement (MOA) and that they are on distribution/notification schedule for threat information (T-2). The MOA should define the relationship and the tenant FP

requirements, especially if the tenant performs a mission or possesses a system that could be at risk to FP threats.

2.7.3. In the event that the host unit does not have an organic intelligence capability and the tenant unit does, tenant intelligence must be prepared to provide FPI support to the host unit; the relationship and requirements defined through MOA.

2.7.4. Tenant units are responsible for providing FPI support to their tenant unit leadership and personnel. Tenant units will:

2.7.4.1. Coordinate with the installation ATO to ensure processes/procedures are in place and documented in the installation ID/AT plan to receive, process, or correlate threat warnings/information. (T-3)

2.7.4.2. Brief tenant staff, aircrews and other appropriate parties on the installation LTA, as required. (T-3)

2.7.4.3. In coordination with local AFOSI Regional offices provide tenant staff, aircrews and other FP customers pre-deployment terrorist and FIE threat information. If needed, the AFOSI Regional offices can seek assistance from the AFOSI ICON. (T-2)

2.7.4.4. Support tenant unit SAVs, ORIs, Vas, UCIs, NSIs, exercises, etc., as required.

2.7.4.5. Document tenant unit activities (e.g., continuity book). (T-2)

2.7.5. While not all the requirements defined in this AFI apply to all tenant units, it should be understood that the role of intelligence in force protection is critical and every effort should be made to guarantee that no gaps exist in support to force protection and the mission.

LARRY D. JAMES, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
and Reconnaissance

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFPD 10-2, Readiness, 30 October 2006

AFPD 14-1, Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations, 2 April 2004

AFPD 14-2, Intelligence Rules and Procedures, 29 November 2007

AFPD 31-1, Integrated Defense, 28 Oct 2011

AFPD 71-1, Criminal Investigations and Counterintelligence, 6 January 2010

AFI 10-245, Antiterrorism (AT), 30 March 2009

AFI 14-104, Oversight of Intelligence Activities, 23 April 2012

AFI 14-105, Unit Intelligence Mission and Responsibilities, 3 June 2002

AFI 14-205, Geospatial Information and Services, 5 May 2010

AFI 14-202, Volume 1, Intelligence Training, 10 March 2008

AFI 14-202, Volume 2, Intelligence Standardization/Evaluation Program, 10 March 2008

AFI 14-202, Volume 3, General Intelligence Rules, 10 March 2008

AFI 16-201, Air Force Foreign Disclosure and Technology Transfer Program, 1 December 2004

AFI 25-201, Support Agreements Procedures, 1 May 2005

AFI 31-201, Security Forces Standards and Procedures, 30 March 2009

AFI 31-101, Integrated Defense (FOUO), 8 October 2009

AFI 32-3001, Explosive Ordnance Disposal (EOD) Program, 2 June 2011

AFI 36-2201, Air Force Training Program, 15 September 2010

AFI 71-101, Volume 4, Counterintelligence, 8 November 2011

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMD 39, *Air Force Office of Special Investigations (OSI)*, 6 July 2011

AFH 31-305, *Security Forces Deployment Planning Handbook*, 26 February 2003

AFTTP 3-10.1, Integrated Base Defense, 20 August 2004

AFDD 3-10, *Force Protection*, 28 July 2011

AFDD 2-0, *Intelligence, Surveillance and Reconnaissance Operations*, 17 July 2007

AFDD 3-27, *Homeland Operations*, 21 March 2006

DoD Directive 2000.12, *DoD Antiterrorism Program*, December 13, 2007

DoD O-2000.12H, *DoD Antiterrorism Handbook*, February 2004

DoD Instruction 2000.16, *DoD Antiterrorism (AT) Standards*, December 8, 2006

DoD 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, March 1, 2010

JP 3-10, *Security Operations in Theater*, February 3, 2010

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

Abbreviations and Acronyms

AF—Air Force

AFOSI—Air Force Office of Special Investigations

AFRC—Air Force Reserve Command

AFSC—Air Force Specialty Code

ANG—Air National Guard

AT—Antiterrorism

ATWG—Antiterrorism Working Group

ATO—Antiterrorism Officer

BDOC—Base Defense Operations Center

BOS—Base Operating Support

C-NAF—Component Numbered Air Force

C2—Command and Control

CBRNE—Chemical, Biological, Radiological, Nuclear, High-yield Explosives

CCIR—Commander's Critical Information Requirement

CE—Civil Engineers

CENTAF—US Central Command Air Forces

CI—Counterintelligence

COA—Course of Action

COCOM—Combatant Command (command authority)

CONUS—Continental United States

CRG—Contingency Response Group

CSAF—Chief of Staff of the Air Force

DET—Detachment (AFOSI)

DFC—Defense Force Commander

DoD—Department of Defense

DTA—Defense Threat Assessment (term has been replaced in DoDI 5240.18, Counterintelligence [CI] Analysis and Production, November 17, 2009, with verbiage related to CI analysis products, i.e., Threat Assessment)

EEI—Essential Elements of Information

EOD—Explosive Ordnance Disposal

FAST—Flyaway Security Team

FIR—Field Investigation Region

FISS—Foreign Intelligence and Security Services

FOUO—For Official Use Only

FP—Force Protection

FPI—Force Protection Intelligence

FPWG—Force Protection Working Group

GEOINT—Geospatial Intelligence

GI&S—Geospatial Information and Services

HAF—Headquarters Air Force

HCS—HUMINT Control System

HHQ—Higher Headquarters

HUMINT—Human Intelligence

IAW—In Accordance With

ID—Integrated Defense

IDRMP—Integrated Defense Risk Management Process

IDWG—Integrated Defense Working Group

IC—Intelligence Community

IED—Improvised Explosive Device

IFC—Intelligence Fusion Cell

IFTU—Intelligence Formal Training Unit

IMA—Individual Mobilization Augmentee

INTREP—Intelligence Report

INTSUM—Intelligence Summary

IO—Intelligence Oversight

ISOPREP—Isolated Personnel Reports

IPOE—Intelligence Preparation of the Operating Environment

ISR—Intelligence, Surveillance and Reconnaissance

LE—Law Enforcement

LOAC—Law of Armed Conflict

MAJCOM—Major Command

MANPADS—Man-Portable Air Defense System

MISREP—Mission Report

MOA—Memorandum of Agreement

NAF—Numbered Air Force

NCO—Non-Commissioned Officer

NSI—Nuclear Surety Inspection

OB—Order of Battle

OCONUS—Outside Continental United States

OPLAN—Operations Plan

OPSEC—Operational Security

ORI—Operational Readiness Inspection

OSS/OSF—Operations Support Squadron/Flight

PIR—Priority Intelligence Requirement

RPG—Rocket Propelled Grenade

RTC—Regional Training Center

SAV—Staff Assistance Visit

SCI—Sensitive Compartmented Information

SF—Security Forces

SME—Subject Matter Expert

SIO—Senior Intelligence Officer

SITREP—Situation Report

SPOTREP—Spot Report

SSO—Special Security Office

T-1—Tier 1

T-2—Tier 2

T-3—Tier 3

TWG—Threat Working Group

UCI—Unit Compliance Inspection

UMD—Unit Manning Document

UTC—Unit Type Code

VA—Vulnerability Assessment

WMD—Weapons of Mass Destruction

Terms

Administrative Control—Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. Also called ADCON. (JP 0-2)

Antiterrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. (JP 1-02)

Antiterrorism Officer (ATO)—The installation, base, regional, facility, or deploying AT advisor charged with managing the AT Program. He/she shall be a graduate of an approved Level II Course and be identified in writing by the installation and/or force commander. Reference AFI 10-245.

Antiterrorism Working Group (ATWG)—The commander's cross-functional working group made up of wing and tenant units. Working group members are responsible for coordinating and providing deliberate planning for all antiterrorism and force protection issues. The ATWG includes representatives from areas across the installation, including civil engineering, intelligence, AFOSI, security forces, public health, bioenvironmental, disaster preparedness, plans, communications, etc.

Base Boundary—A line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operation between adjacent units, formation, or areas. (JP 1-02)

Base Defense Operations Center (BDOC)—A command and control facility established by the base commander to serve as the focal point for base security and defense. It plans, directs, integrates, coordinates, and controls all base defense efforts and coordinates and integrates into area security operations with the rear area operations center/rear tactical operations center. Reference AFI 31-101.

Base Security Zone—The battle space from which the enemy can launch an attack against base personnel and resources or aircraft approaching/departing the base. (AFTTP 3-10.2)

Battle Space—The commander's conceptual view of the area and factors which he/she must understand to successfully apply combat power, protect the force, and complete the mission. It encompasses all applicable aspects of air, sea, space, and land operations that the commander must consider in planning and executing military operations. The battle space dimensions can change over time as the mission expands or contracts according to operational objectives and force composition. Battle space provides the commander a mental forum for analyzing and selecting courses of action for employing military forces in relationship to time, tempo, and depth.

Commander's Critical Information Requirement (CCIR)—An information requirement identified by the commander as being critical to facilitating timely decision-making. The two key elements are friendly force information requirements and priority intelligence requirements.

Contingency Response Group (CRG)—An AF capability with effects that span the joint force, the CRG serves as the first of five force modules to assess and open air bases to extend the reach of air and space forces. They provide combatant commanders with initial Airbase Opening and air mobility support capability during wartime, contingency, or other USTRANSCOM/AMC directed missions. CRG extend air mobility operations worldwide by deploying task organized mobility teams capable of airbase assessment, initial C2, cargo and passenger handling, in-transit visibility, quick-turn aircraft maintenance, self-protection security, air traffic control, and airfield operations.

Counterintelligence (CI)—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. In this AFI, CI specifically refers to information about threats to AF installations gathered through activities conducted by the AFOSI or other service and national CI organizations. CI analyzes the threats posed by foreign intelligence and security services and the intelligence activities of non-state actors such as organized crime, terrorist groups, drug traffickers, and the insider threat. CI analysis incorporates all-source information and the results of CI investigations and operations to support a multidiscipline analysis of the force protection threat.

Critical Asset Risk Management (CARM) Program—Formerly known as the Critical Infrastructure program, CARM is a mission assurance, risk-management-based program that assures the AF's ability to execute missions and capabilities essential to planning, mobilizing, deploying, executing and sustaining military operations that encompass Combatant Command operational and AF Title 10 United States Code (U.S.C.) missions and capabilities.

Defense Force Commander (DFC)—The DFC directs the planning and execution of base defense operations and serves as the Installation Commander's primary advisor for ID. On AF installations, the SF squadron commander is the DFC. On installations with more than one SF squadron, the DFC is the SF commander responsible for installation security. In addition to SF permanently assigned to the DFC, the DFC exercises TACON of the ID mission and supporting forces. The tactical role of the DFC does not grant him/her administrative control (ADCON) authority of supporting ID forces; however, the DFC's tactical role serves to ensure unity of effort, cohesive communication, deconfliction of issues, and to lessen the likelihood of fratricide.

Defense Threat Assessment (DTA)—An all-source assessment of threats to an installation. AFOSI is responsible for the DTA. Reference DoD message, *Standardized DoD Threat Assessment*, 22 Dec 03; AFOSI Manual 71-144 Volume 7, *CI Collections, Analysis and Production*.

Essential Elements of Information—The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.

Flyaway Security Team (FAST)—See Phoenix Ravens

Force Protection (FP)—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include Active Duty, AFRC, ANG, DoD civilians, contractors, and family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. (JP 1-02) **Note:** The AF definition in AFDD 3-10 deviates as: The process of detecting threats and hazards to the AF and its mission, and applying measures to deter, pre-empt, negate or mitigate them based on an acceptable risk; this modified definition does not expand the Intel support mission to include all hazards (e.g., EM, bio-medical, infrastructure, weather), it is only provided for understanding and clarity.

Force Protection Information—Fused information from FP sources (CI, SF, Intel, etc.) that provides the best available picture of the intents and capabilities of terrorists or extremists, criminal entities and enterprises, FISS, opposing military forces, and in certain instances, environmental/medical hazards, infrastructure vulnerabilities, and insider threats.

Force Protection Intelligence (FPI)—Analyzed, all-source intelligence information that when integrated, or fused with other FP information provides an assessment of the threats to DoD missions, people or resources. FPI is proactive and drives FP decisions in support of commander's intent.

Force Protection Program—Commander's program designed to protect Service members, civilian employees, family members, facilities, information and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services and supported by intelligence, counterintelligence and other security programs.

Foreign Disclosure—Oral or visual transmission of information through approved channels to authorized representative of a foreign government.

Geospatial Intelligence (GEOINT)—The exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence and geospatial information. (JP 2-03)

Information—Facts, data, or instructions in any medium or form.

Integrated Defense—The application of active and passive defense measures, employed across the legally-defined ground dimension of the operational environment, to mitigate potential risks and defeat adversary threats to AF operations. As an AF-wide responsibility, effective ID helps ensure effective FP. Security of resources and personnel, in garrison or deployed, is an inherent command responsibility and requires active participation of all Airman, regardless of AF specialty, rank or position for mission success.

Intelligence—The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (JP 1-02)

Intelligence Fusion Cell (IFC)—The IFC is a proactive action group, either collocated or virtually connected, whereby the Security Forces Staff coordinates with subject matter experts (SMEs) from the Intelligence and AFOSI communities to collaborate and conduct IPOE; the goal being to leverage information to support the timely identification of indicators and warnings of emerging localized threats. The IFC and its products are the primary information sources that directly support the DFC in making immediate, proactive decisions for ID planning.

Intelligence Oversight (IO)—Program developed to ensure that government entities conducting intelligence activities do not infringe on or violate the rights of US persons and operate within assigned legal parameters. Reference AFI 14-104, *Oversight of Intelligence Activities*.

Intelligence Preparation of the Operating Environment (IPOE)—A systematic, continuous process of analyzing the threat and environment in a specific geographic area. It is designed to support staff estimates and military decision-making.

Law Enforcement Information—Information provided by any agency chartered and empowered to enforce laws in CONUS; a state or political subdivision of the US; a territory, possession or political subdivision of the US; or within the borders of a host nation. Law Enforcement Sensitive (LES) information specifically refers to unclassified FOUO information that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence and the integrity of pretrial investigative reports.

Measurement and Signature Intelligence (MASINT)—Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydro-magnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. (JP 2-0)

Operational Control—Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training.

Phoenix Ravens/Flyaway Security Team (FAST)—The Phoenix Ravens and FAST Programs are designed to ensure adequate protection for aircraft transiting airfields where security is unknown or deemed inadequate to counter local threats. Teams of two to four specially trained and equipped Security Forces personnel deploy to deter, detect, and counter threats to personnel/aircraft by performing a variety of duties (e.g., close-in aircraft security, advising

aircrews on FP measures, accomplishing airfield assessments to document existing security measures and vulnerabilities).

Priority Intelligence Requirement (PIR)—Intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making.

Terrorism—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorism Threat Level—An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of four elements: operational capability, intentions, activity and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT and HIGH. Threat levels should not be confused with force protection conditions. Threat level assessments are provided to senior leaders to assist them in determining the appropriate local force protection condition. Department of State and Department of Homeland Security also make threat assessments, which may differ from those determined by Department of Defense.

Threat Assessment—Analytic products produced by the OSI to address the threat posed by espionage, international terrorism, subversion, sabotage, assassination, and covert activities. This includes other activities that have a foreign intelligence entity (FIE) nexus. Reference DoD Instruction 5240.18, Counterintelligence (CI) Analysis and Production, November 17, 2009.

Threat Working Group (TWG)—An advisory body that meets at least quarterly or more frequently to develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries. TWG membership is determined by the commander and typically is anchored by ATO, AFOSI, Intel, and Security Forces, but may include members of the staff such as Medical, Communications, Civil Engineering and Operations tenant unit representatives; and appropriate representation from local, State, Federal, and host-nation law enforcement agencies as needed depending upon the threat. Further guidance for the TWG is found in AFI 10-245, DoDI 2000.16, DoD Antiterrorism (AT) Standards, October 2, 2006.

US Persons—The term “United States Person” applies to the following: 1. A United States citizen; 2. An alien known by the DoD intelligence component concerned to be a permanent resident alien. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence; 3. An unincorporated association substantially composed mostly of United States citizens or permanent resident aliens; 4. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

Vulnerability Assessment—A Department of Defense-, command- or unit-level evaluation of the extent to which an installation, unit, exercise, port, ship, residence, facility, or other site would be vulnerable to a terrorist attack. Identifies areas that could be improved to withstand, mitigate, or deter acts of violence or terrorism.